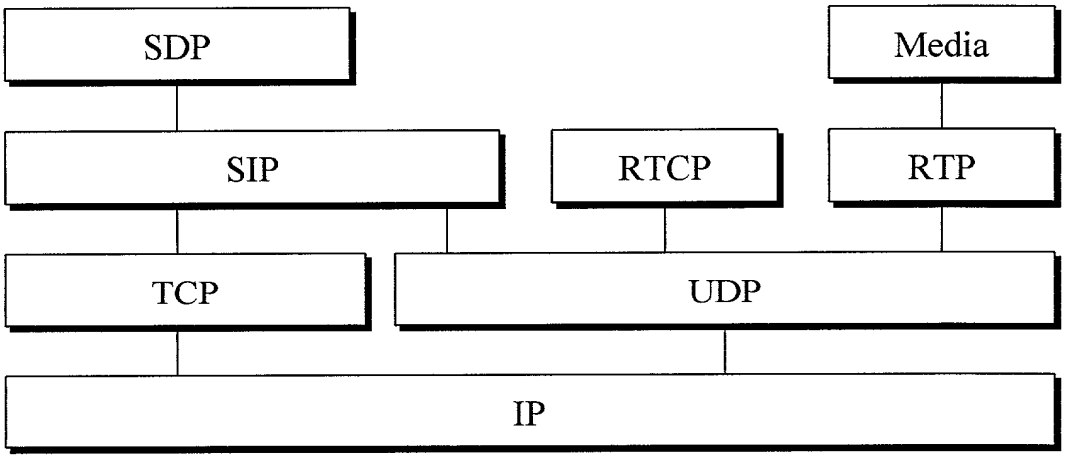
SDP
Media
SIP
RTCP
RTP
TCP
UDP
IP

FIG. 1

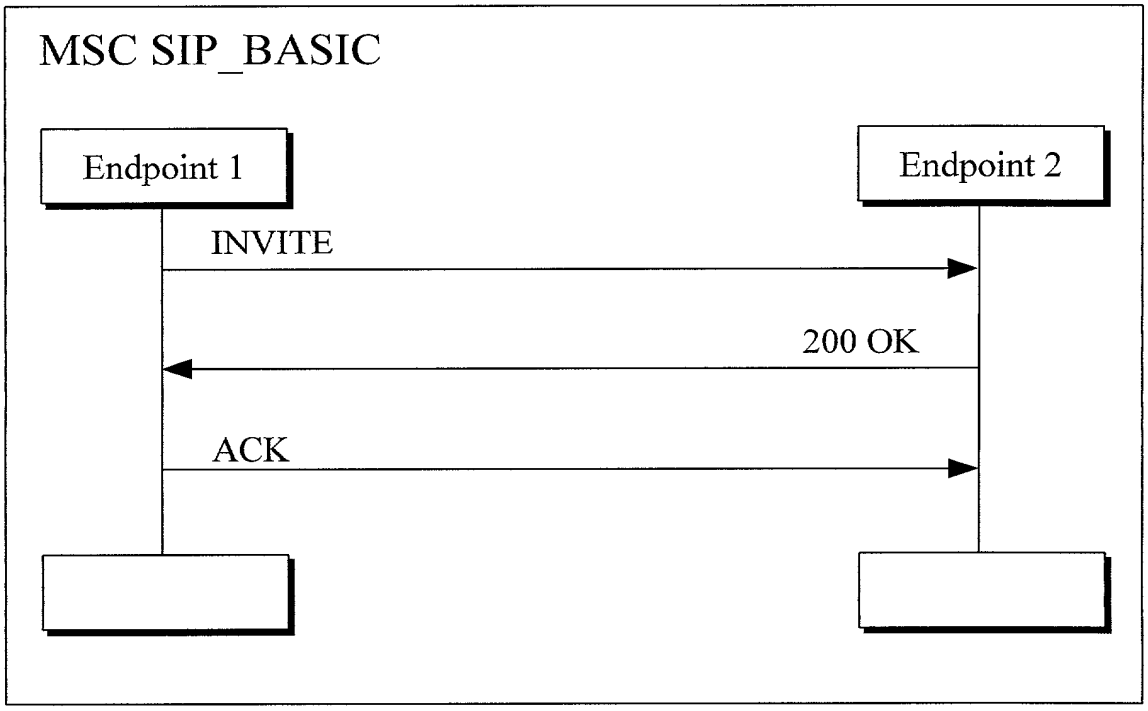
MSC SIP_BASIC
Endpoint 1
Endpoint 2
INVITE
200 OK
ACK

FIG. 2

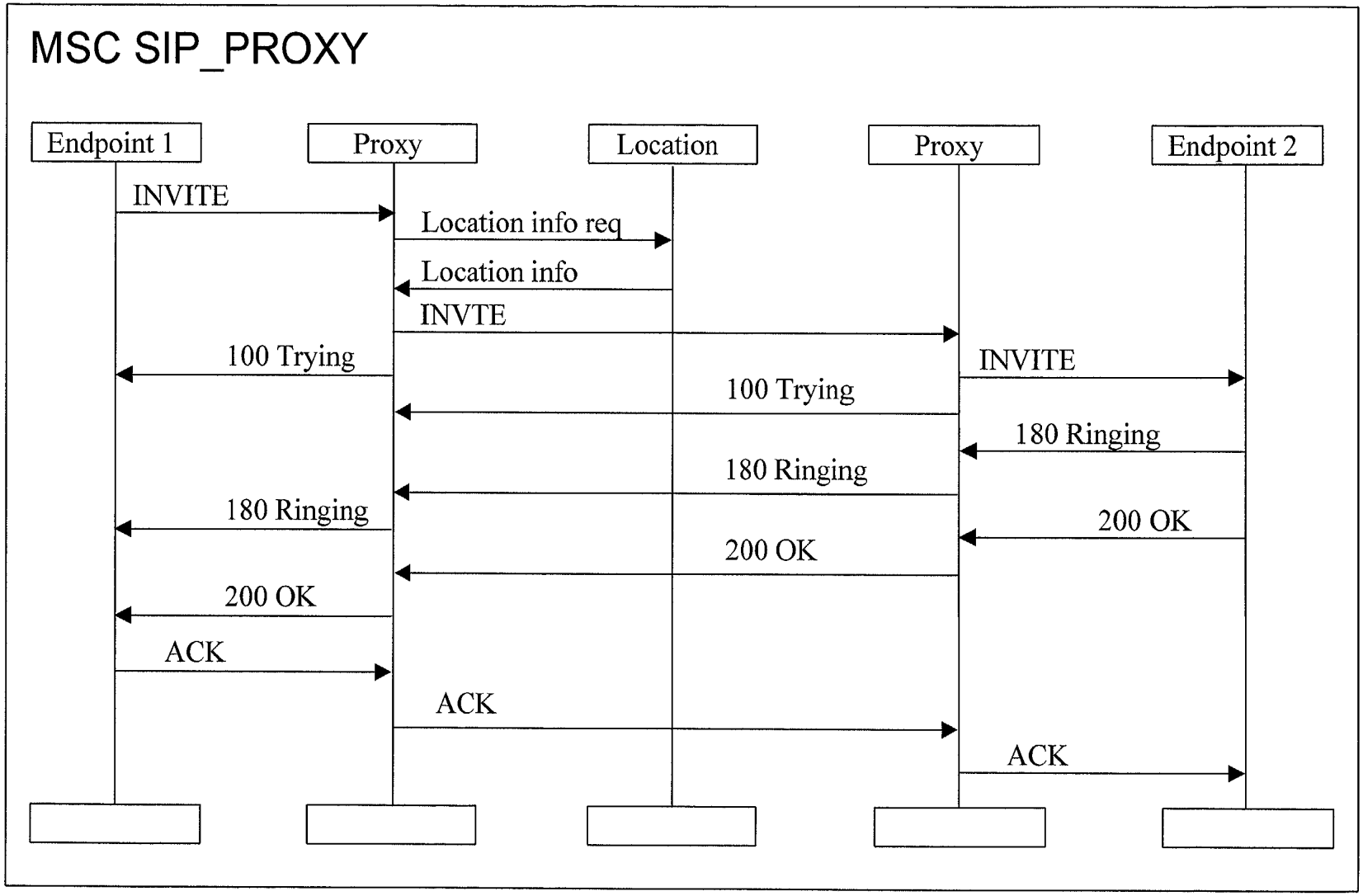
MSC SIP_PROXY
Endpoint 1
Proxy
Location
Proxy
Endpoint 2
INVITE
Location info req
Location info
INVTE
100 Trying
INVITE
100 Trying
180 Ringing
180 Ringing
180 Ringing
200 OK
200 OK
200 OK
ACK
ACK
ACK

FIG. 3

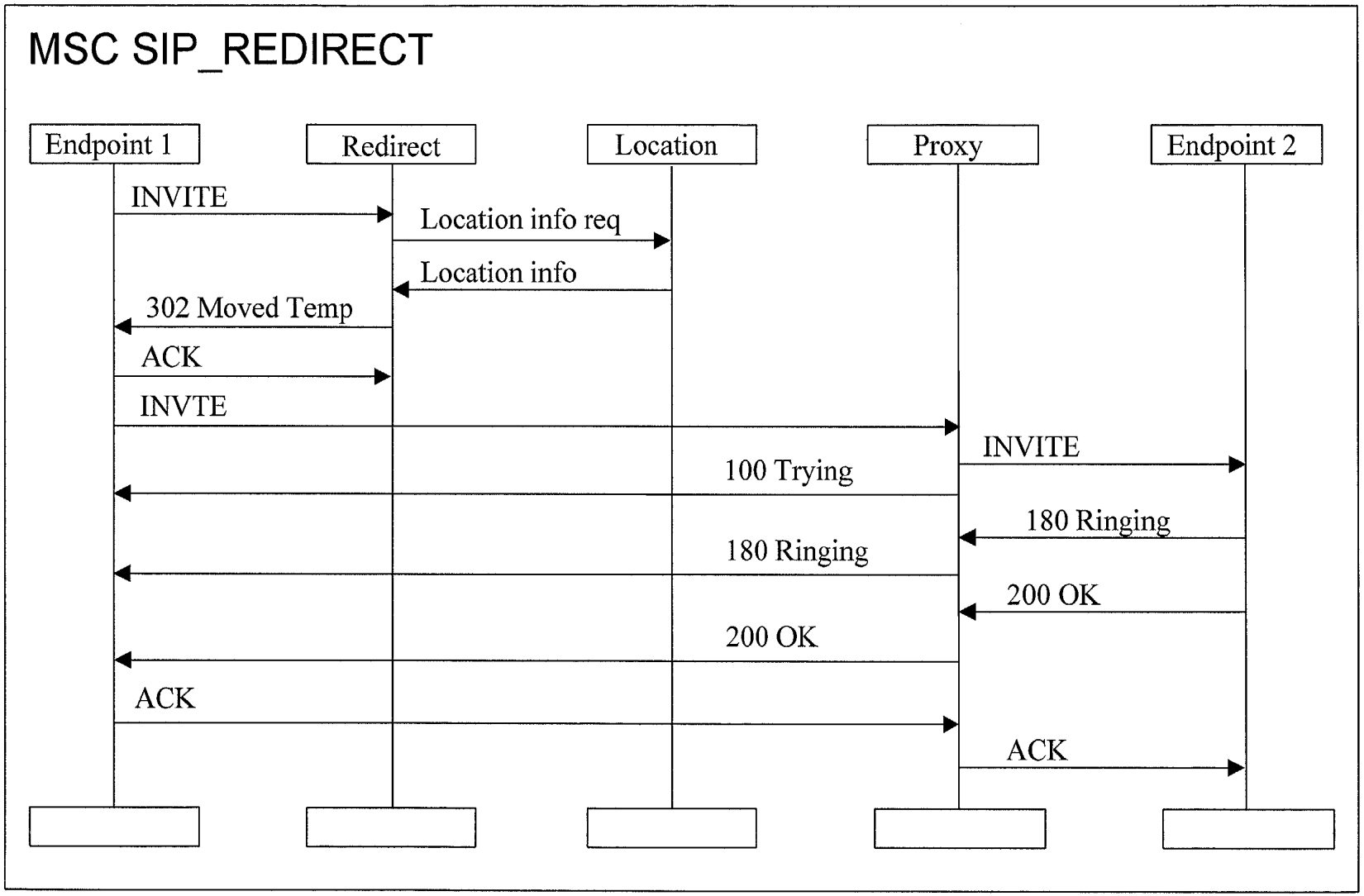
MSC SIP_REDIRECT
Endpoint 1
Redirect
Location
Proxy
Endpoint 2
INVITE
Location info req
Location info
302 Moved Temp
ACK
INVTE
INVITE
100 Trying
180 Ringing
180 Ringing
200 OK
200 OK
ACK
ACK

FIG. 4

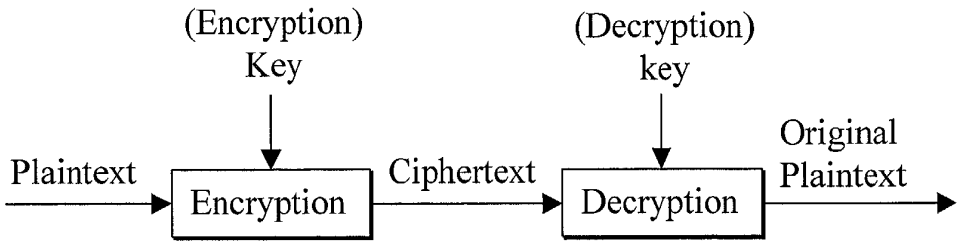
(Encryption)
Key
(Decryption)
key
Plaintext
Encryption
Ciphertext
Decryption
Original
Plaintext

FIG. 5

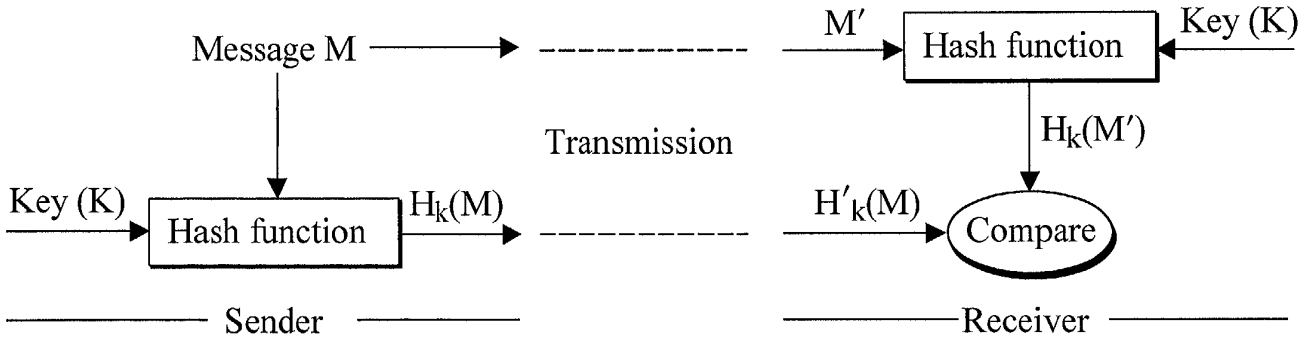
Message M
M′
Hash function
Key (K)
Transmission
Hk(M′)
Key (K)
Hash function
Hk(M)
H′k(M)
Compare
Sender
Receiver

FIG. 6

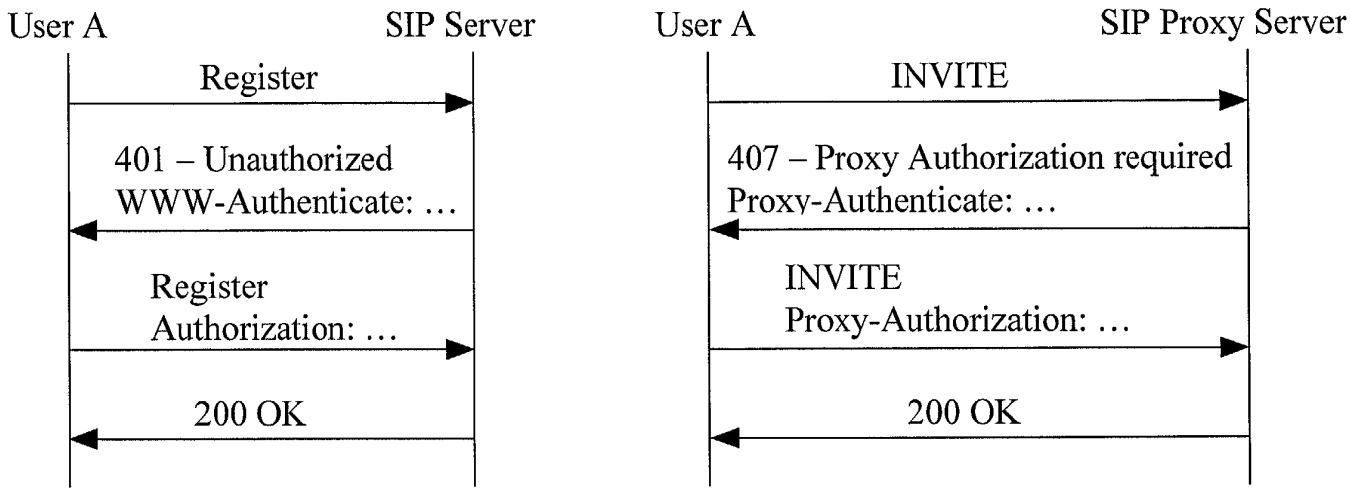
User A
SIP Server
Register
401 – Unauthorized
WWW-Authenticate: …
Register
Authorization: …
200 OK
User A
SIP Proxy Server
INVITE
407 – Proxy Authorization required
Proxy-Authenticate: …
INVITE
Proxy-Authorization: …
200 OK

FIG. 7

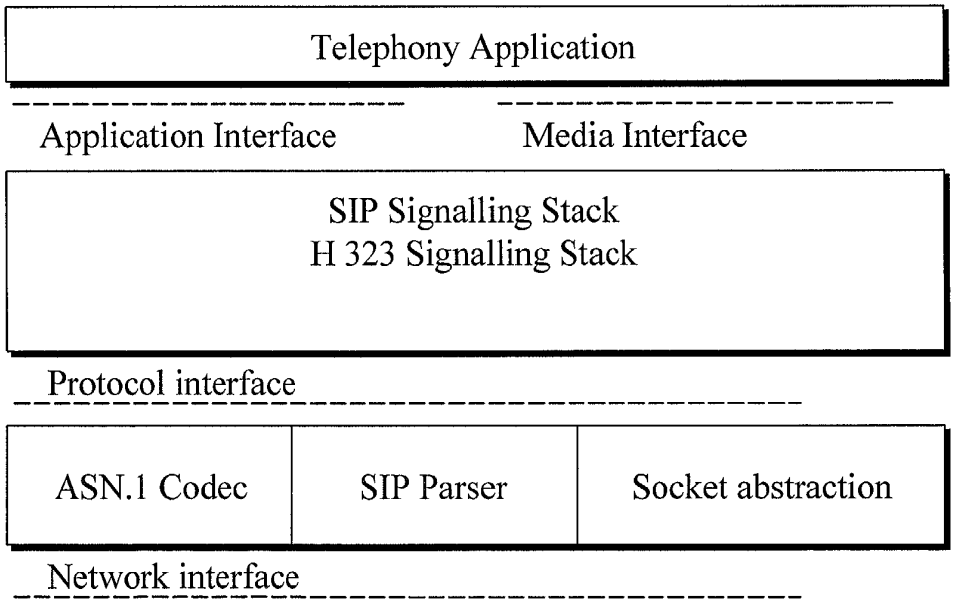
Telephony Application
Application Interface
Media Interface
SIP Signalling Stack
H 323 Signalling Stack
Protocol interface
ASN.1 Codec
SIP Parser
Socket abstraction
Network interface

FIG. 8

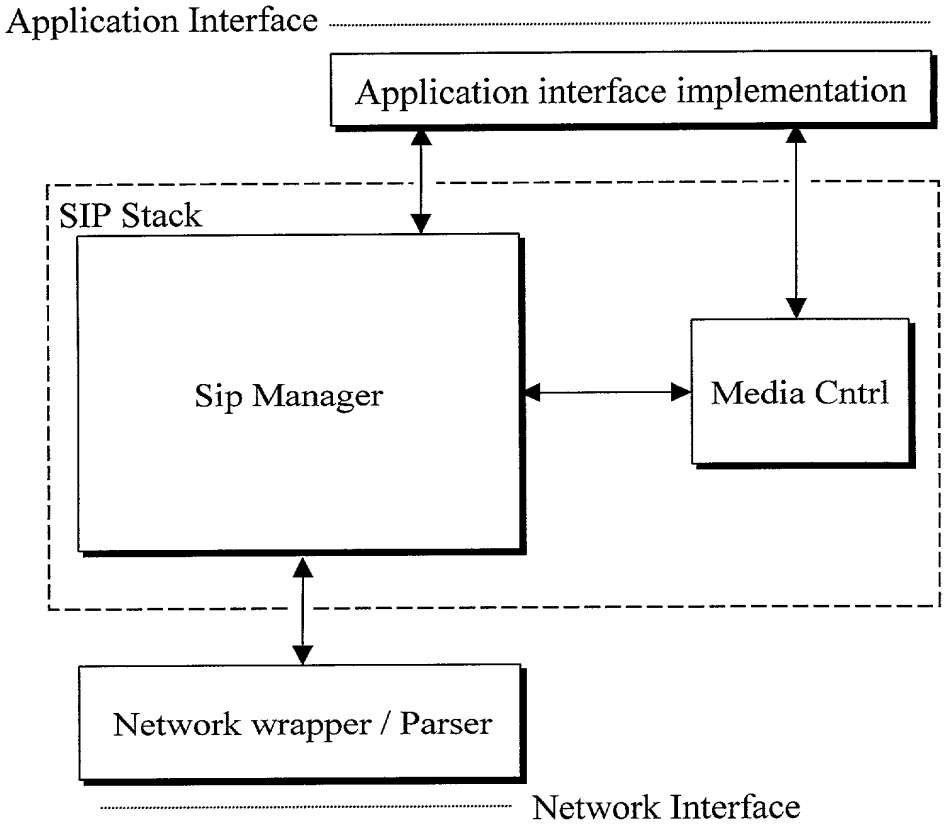

FIG. 9

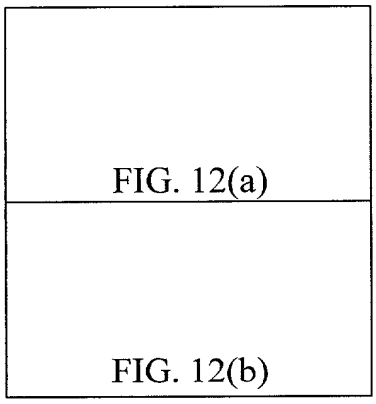

FIG. 12

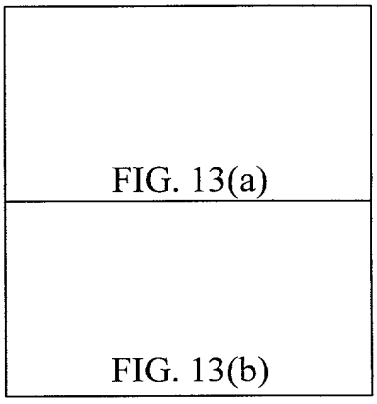

FIG. 13

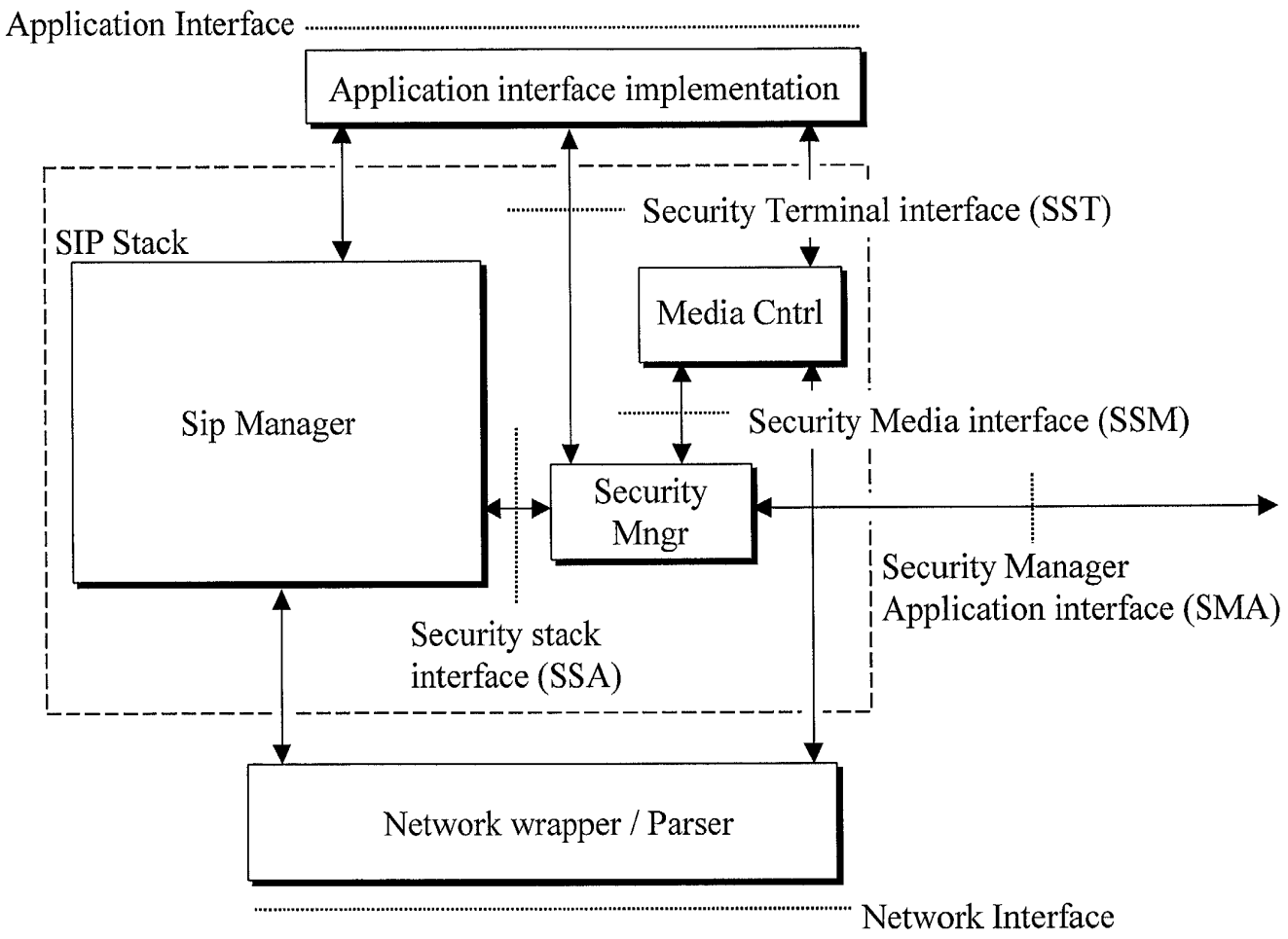
Application Interface
Application interface implementation
Security Terminal interface (SST)
SIP Stack
Media Cntrl
Sip Manager
Security Media interface (SSM)
Security
Mngr
Security Manager
Application interface (SMA)
Security stack
interface (SSA)
Network wrapper / Parser
Network Interface

FIG. 10

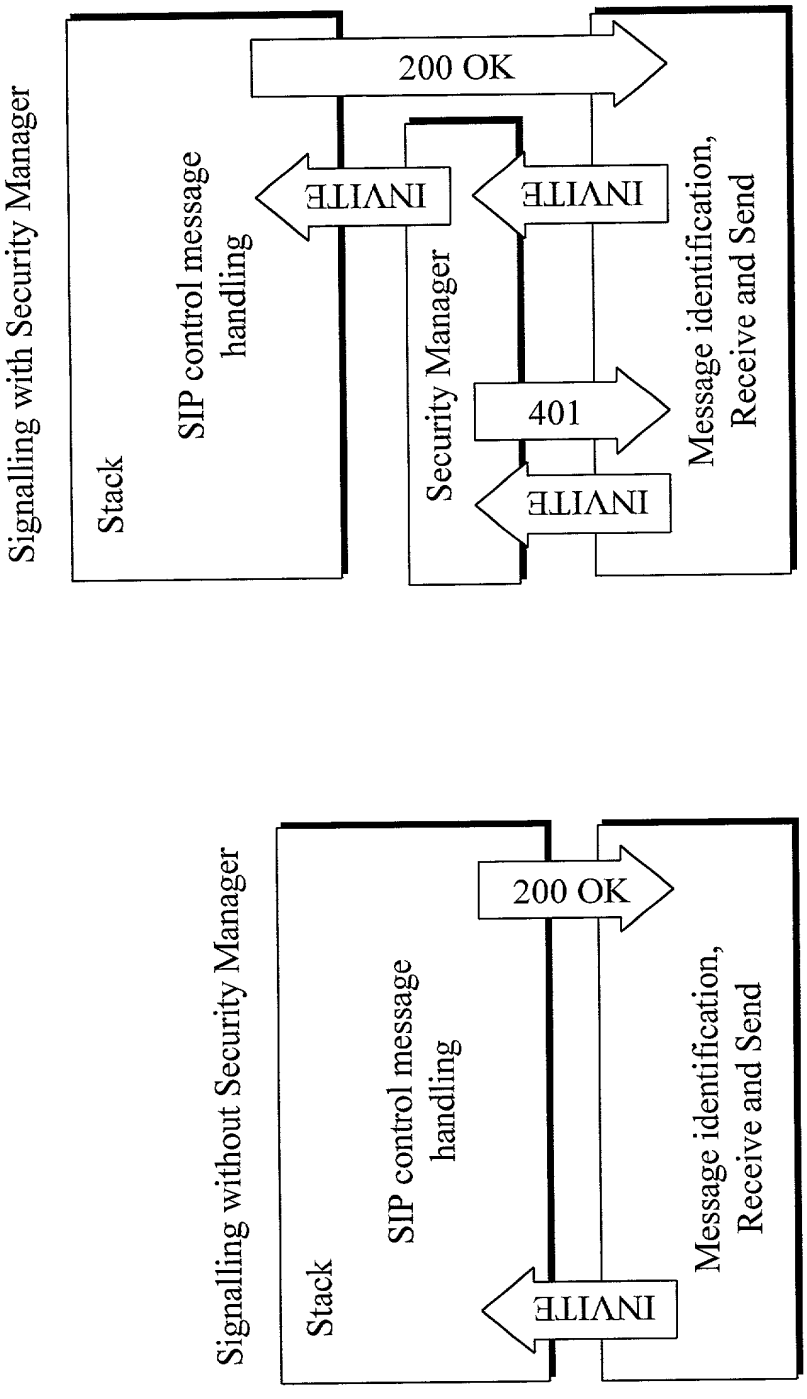
Signalling with Security Manager
Stack
SIP control message handling
Security Manager
Message identification, Receive and Send
INVITE
INVITE
200 OK
401
INVITE
Signalling without Security Manager
Stack
SIP control message handling
Message identification, Receive and Send
INVITE
200 OK

FIG. 11

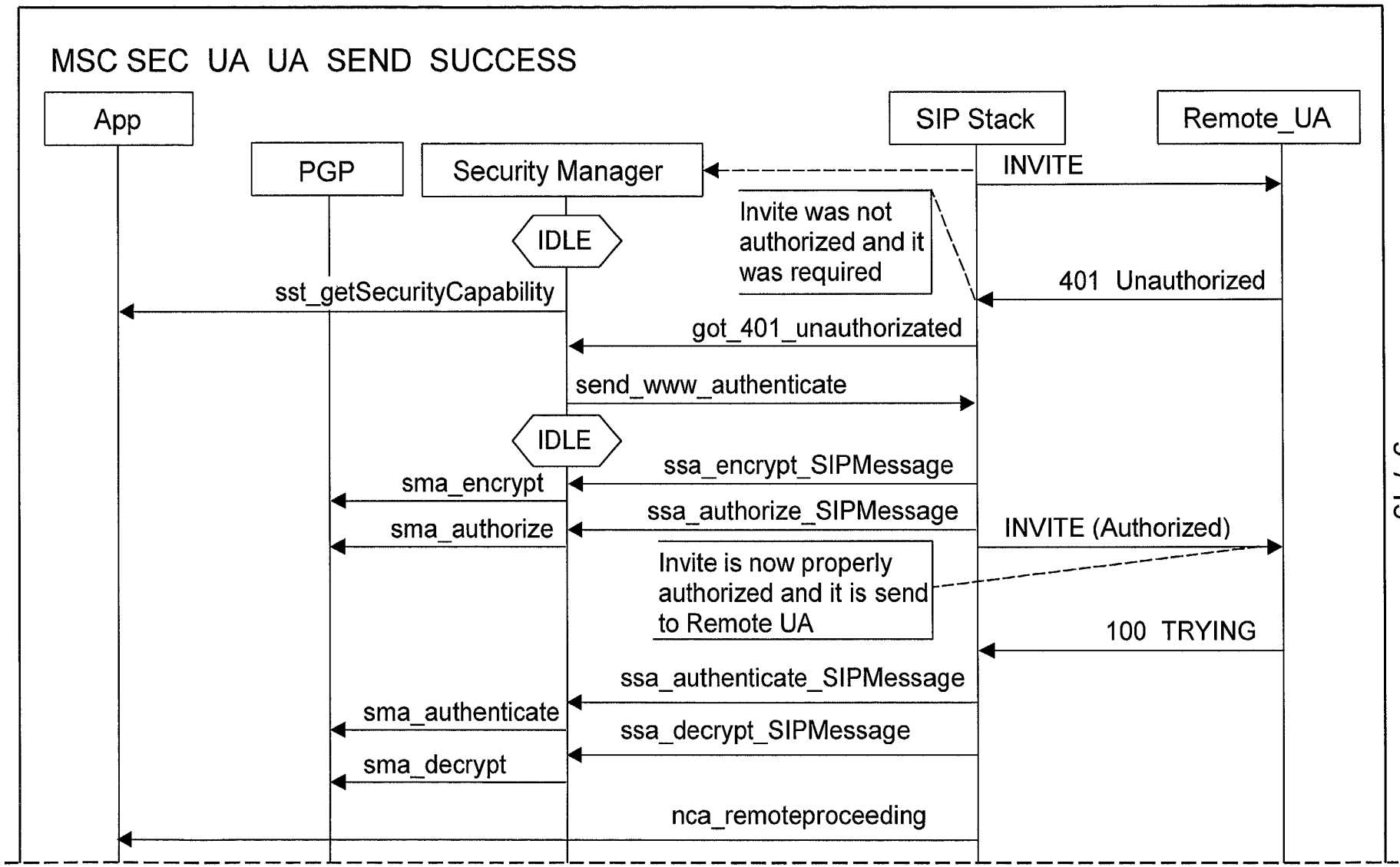
MSC SEC UA UA SEND SUCCESS
App
PGP
Security Manager
SIP Stack
Remote_UA
INVITE
Invite was not authorized and it was required
IDLE
401 Unauthorized
sst_getSecurityCapability
got_401_unauthorizated
send_www_authenticate
IDLE
ssa_encrypt_SIPMessage
sma_encrypt
ssa_authorize_SIPMessage
sma_authorize
INVITE (Authorized)
Invite is now properly authorized and it is send to Remote UA
100 TRYING
ssa_authenticate_SIPMessage
sma_authenticate
ssa_decrypt_SIPMessage
sma_decrypt
nca_remoteproceeding

FIG. 12(a)

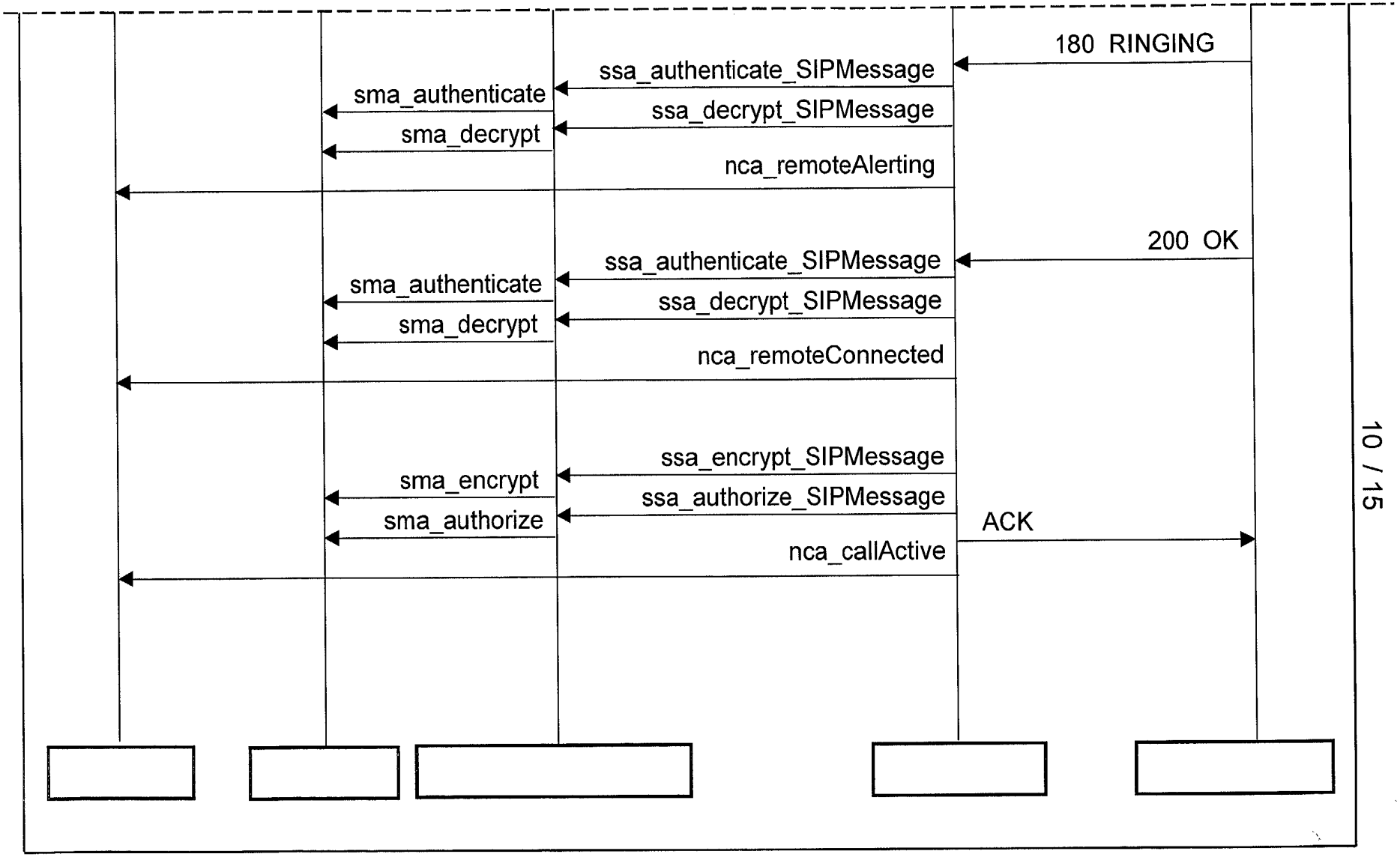
180 RINGING
ssa_authenticate_SIPMessage
sma_authenticate
ssa_decrypt_SIPMessage
sma_decrypt
nca_remoteAlerting
200 OK
ssa_authenticate_SIPMessage
sma_authenticate
ssa_decrypt_SIPMessage
sma_decrypt
nca_remoteConnected
ssa_encrypt_SIPMessage
sma_encrypt
ssa_authorize_SIPMessage
sma_authorize
ACK
nca_callActive

FIG. 12(b)

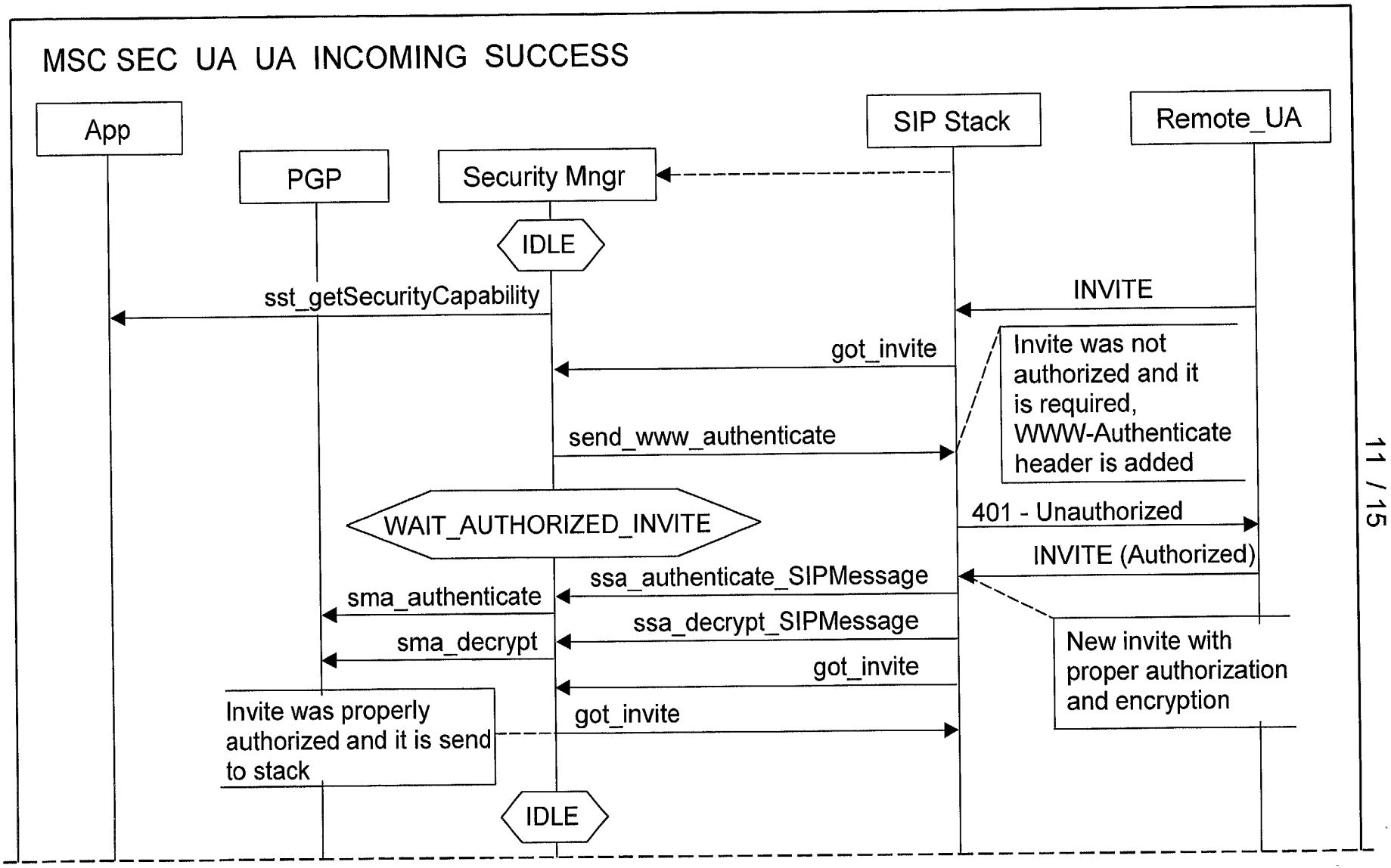
MSC SEC UA UA INCOMING SUCCESS
App
PGP
Security Mngr
SIP Stack
Remote_UA
IDLE
sst_getSecurityCapability
INVITE
got_invite
Invite was not authorized and it is required, WWW-Authenticate header is added
send_www_authenticate
WAIT_AUTHORIZED_INVITE
401 - Unauthorized
INVITE (Authorized)
ssa_authenticate_SIPMessage
sma_authenticate
ssa_decrypt_SIPMessage
sma_decrypt
New invite with proper authorization and encryption
got_invite
Invite was properly authorized and it is send to stack
got_invite
IDLE

FIG. 13(a)

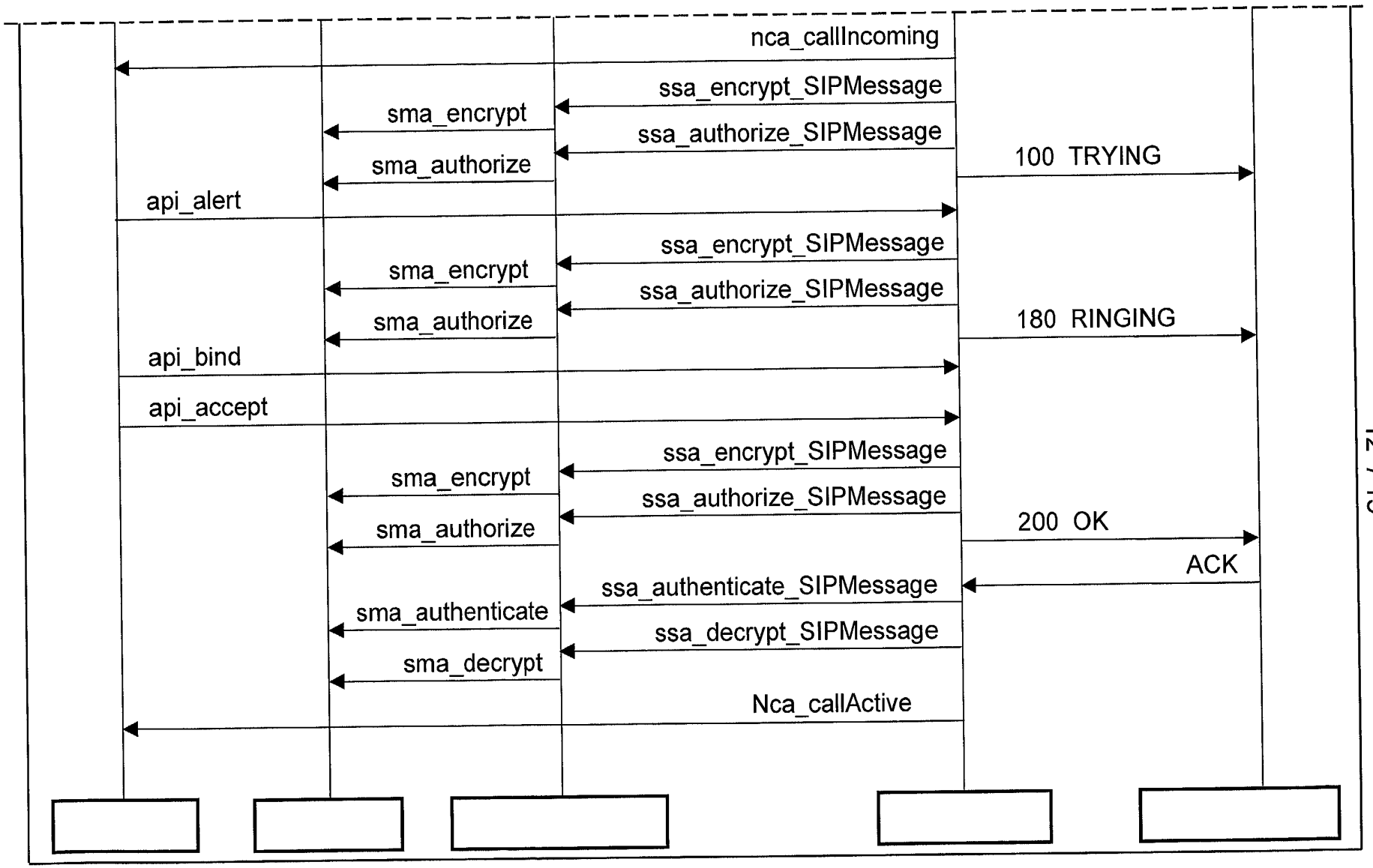
nca_callIncoming
ssa_encrypt_SIPMessage
sma_encrypt
ssa_authorize_SIPMessage
100 TRYING
sma_authorize
api_alert
ssa_encrypt_SIPMessage
sma_encrypt
ssa_authorize_SIPMessage
180 RINGING
sma_authorize
api_bind
api_accept
ssa_encrypt_SIPMessage
sma_encrypt
ssa_authorize_SIPMessage
200 OK
sma_authorize
ACK
ssa_authenticate_SIPMessage
sma_authenticate
ssa_decrypt_SIPMessage
sma_decrypt
Nca_callActive

FIG. 13(b)

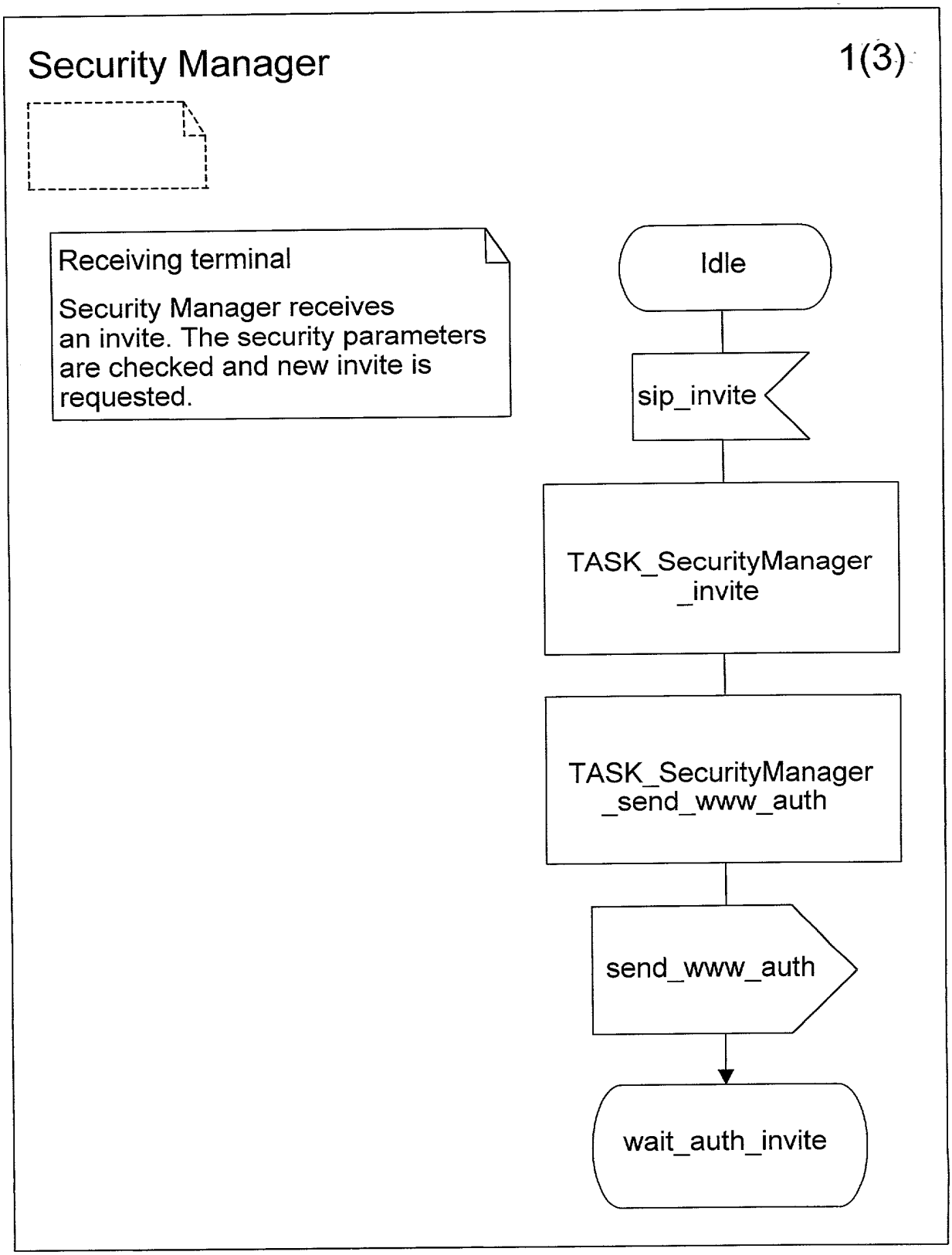
Security Manager
1(3)
Receiving terminal
Security Manager receives an invite. The security parameters are checked and new invite is requested.
Idle
sip_invite
TASK_SecurityManager _invite
TASK_SecurityManager _send_www_auth
send_www_auth
wait_auth_invite

FIG. 14(a)

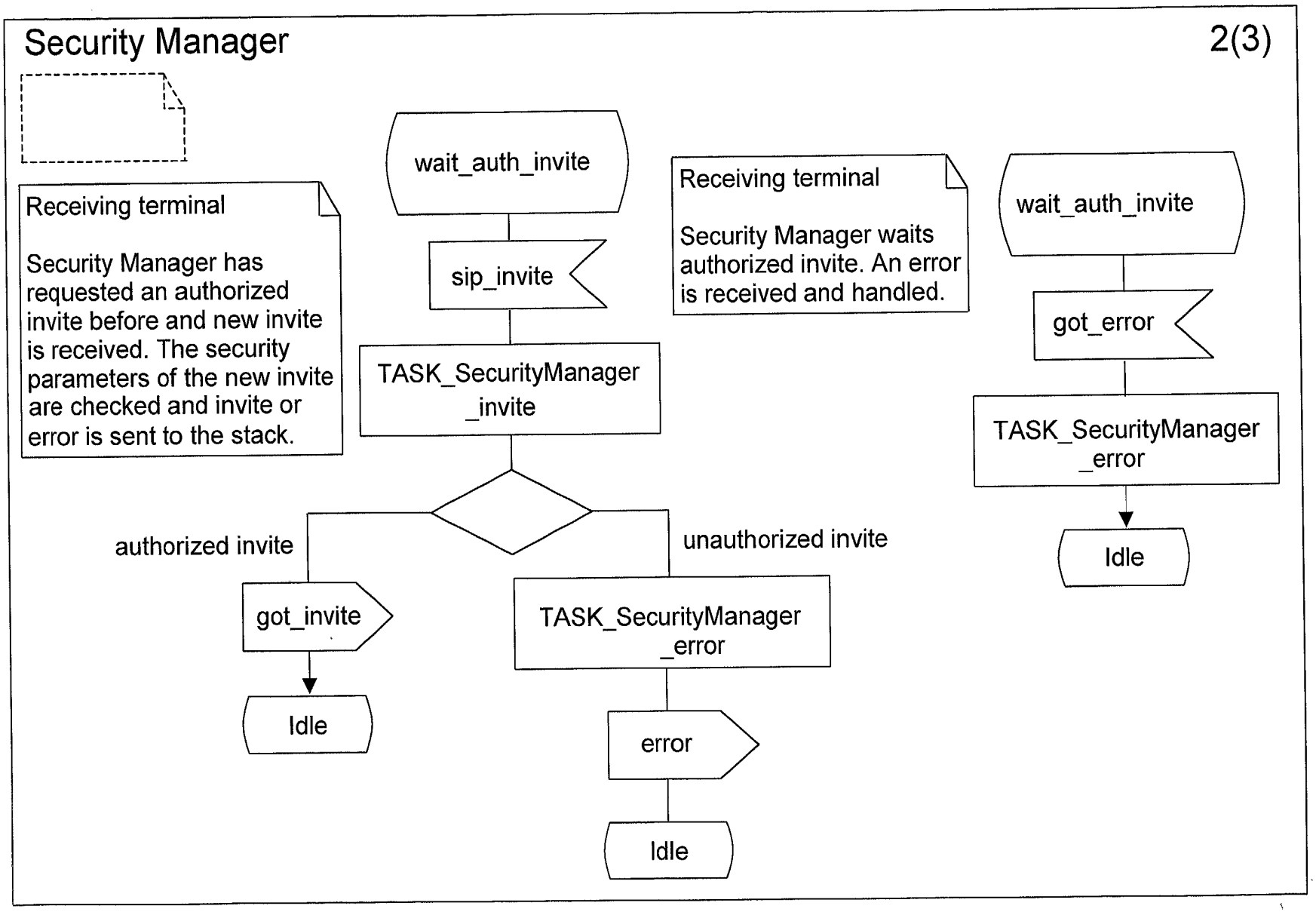
Security Manager
2(3)
Receiving terminal
Security Manager has requested an authorized invite before and new invite is received. The security parameters of the new invite are checked and invite or error is sent to the stack.
wait_auth_invite
sip_invite
TASK_SecurityManager _invite
authorized invite
unauthorized invite
got_invite
Idle
TASK_SecurityManager _error
error
Idle
Receiving terminal
Security Manager waits authorized invite. An error is received and handled.
wait_auth_invite
got_error
TASK_SecurityManager _error
Idle

FIG. 14(b)

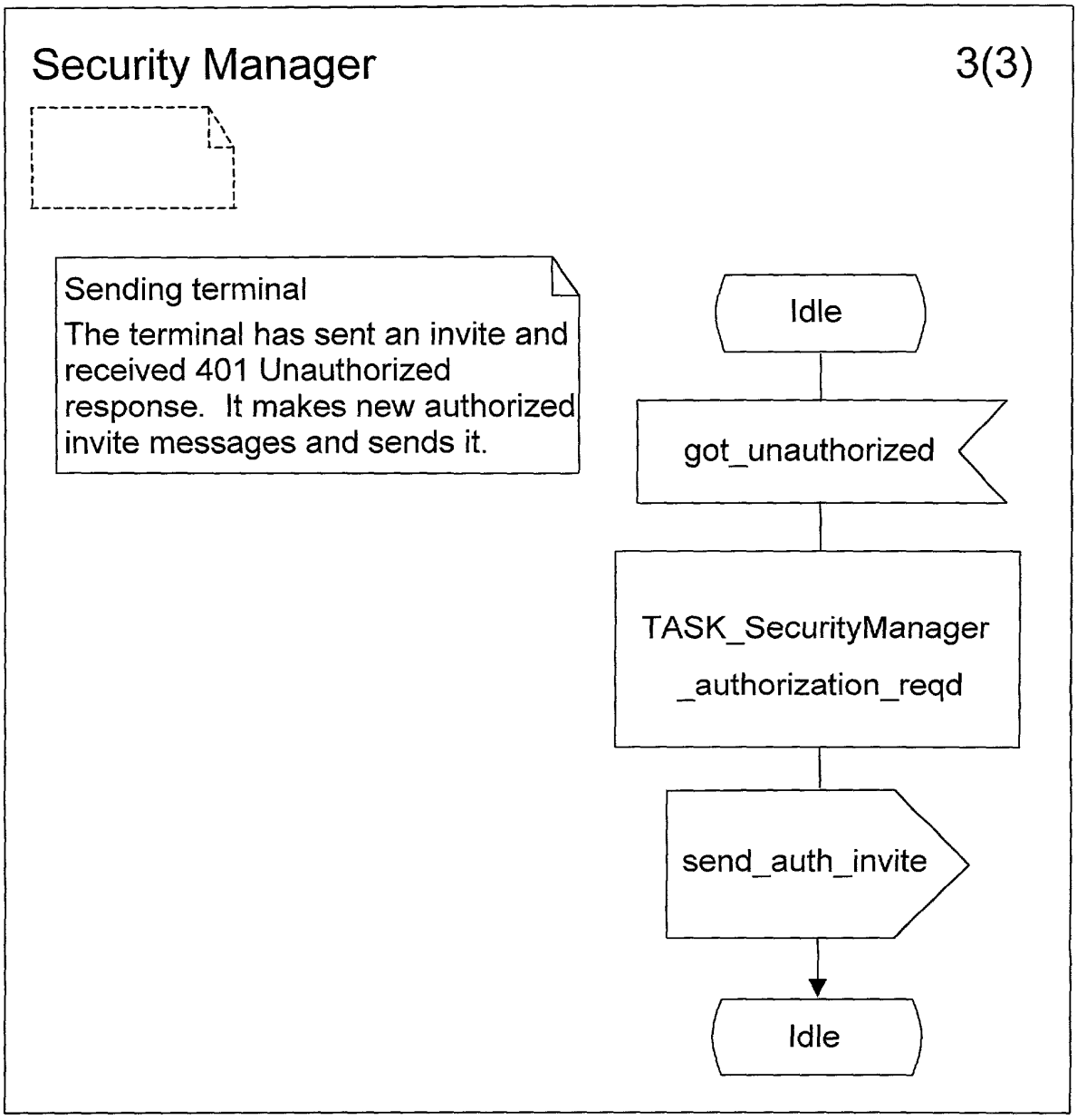
Security Manager
3(3)
Sending terminal
The terminal has sent an invite and received 401 Unauthorized response. It makes new authorized invite messages and sends it.
Idle
got_unauthorized
TASK_SecurityManager
_authorization_reqd
send_auth_invite
Idle

FIG. 14(c)